FIG. 1

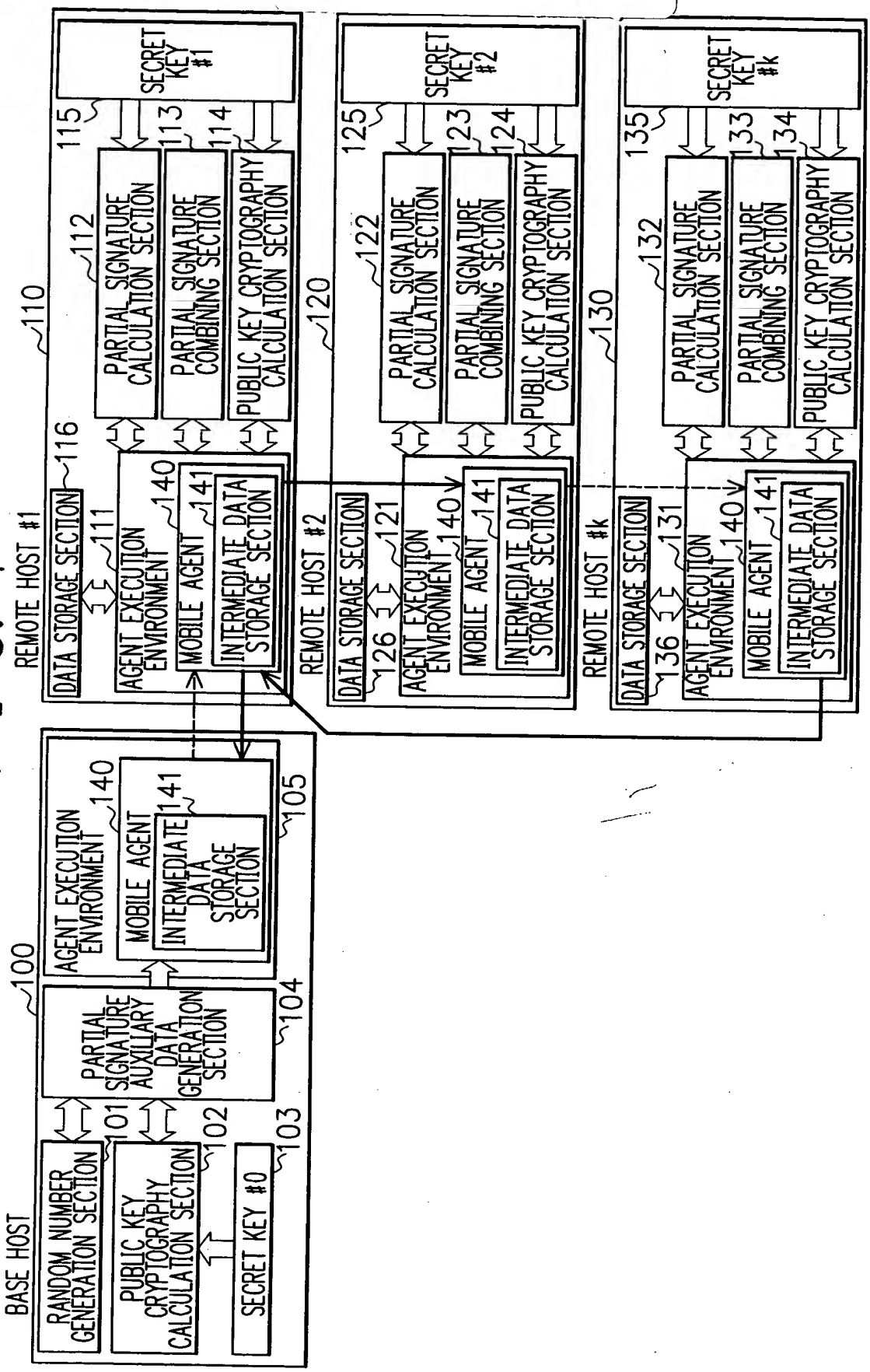

BASE HOST
100
RANDOM NUMBER GENERATION SECTION
101
PUBLIC KEY CRYPTOGRAPHY CALCULATION SECTION
102
SECRET KEY #0
103
PARTIAL SIGNATURE AUXILIARY DATA GENERATION SECTION
104
AGENT EXECUTION ENVIRONMENT
140
MOBILE AGENT
141
INTERMEDIATE DATA STORAGE SECTION
105
REMOTE HOST #1
110
DATA STORAGE SECTION
116
111
AGENT EXECUTION ENVIRONMENT
140
MOBILE AGENT
141
INTERMEDIATE DATA STORAGE SECTION
PARTIAL SIGNATURE CALCULATION SECTION
112
PARTIAL SIGNATURE COMBINING SECTION
113
PUBLIC KEY CRYPTOGRAPHY CALCULATION SECTION
114
SECRET KEY #1
115
REMOTE HOST #2
120
DATA STORAGE SECTION
126
121
AGENT EXECUTION ENVIRONMENT
140
MOBILE AGENT
141
INTERMEDIATE DATA STORAGE SECTION
PARTIAL SIGNATURE CALCULATION SECTION
122
PARTIAL SIGNATURE COMBINING SECTION
123
PUBLIC KEY CRYPTOGRAPHY CALCULATION SECTION
124
SECRET KEY #2
125
REMOTE HOST #k
130
DATA STORAGE SECTION
136
131
AGENT EXECUTION ENVIRONMENT
140
MOBILE AGENT
141
INTERMEDIATE DATA STORAGE SECTION
PARTIAL SIGNATURE CALCULATION SECTION
132
PARTIAL SIGNATURE COMBINING SECTION
133
PUBLIC KEY CRYPTOGRAPHY CALCULATION SECTION
134
SECRET KEY #k
135

FIG. 2

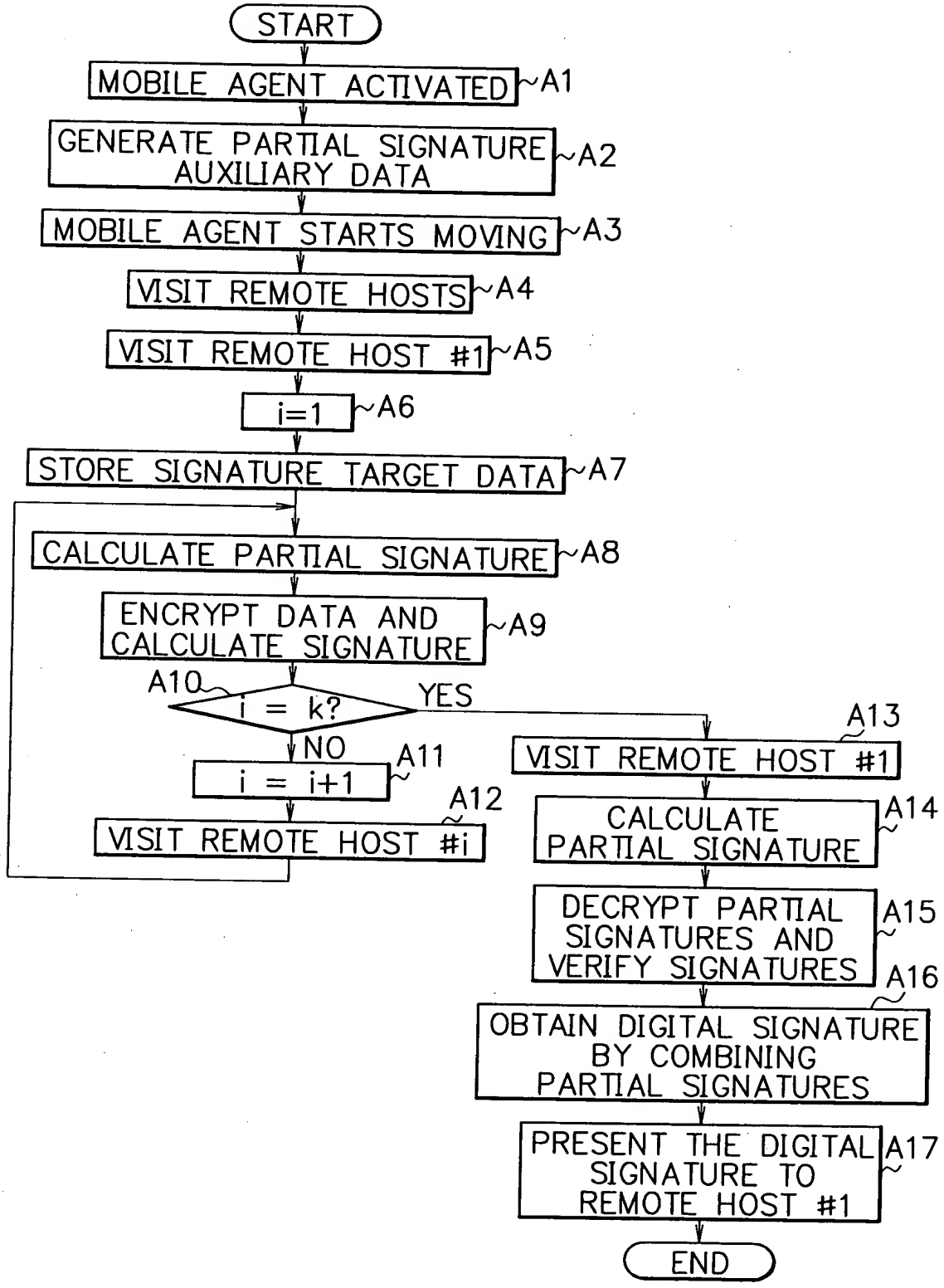

START
MOBILE AGENT ACTIVATED
A1
GENERATE PARTIAL SIGNATURE AUXILIARY DATA
A2
MOBILE AGENT STARTS MOVING
A3
VISIT REMOTE HOSTS
A4
VISIT REMOTE HOST #1
A5
i=1
A6
STORE SIGNATURE TARGET DATA
A7
CALCULATE PARTIAL SIGNATURE
A8
ENCRYPT DATA AND CALCULATE SIGNATURE
A9
A10
i = k?
YES
NO
A11
i = i+1
A12
VISIT REMOTE HOST #i
A13
VISIT REMOTE HOST #1
CALCULATE PARTIAL SIGNATURE
A14
DECRYPT PARTIAL SIGNATURES AND VERIFY SIGNATURES
A15
A16
OBTAIN DIGITAL SIGNATURE BY COMBINING PARTIAL SIGNATURES
PRESENT THE DIGITAL SIGNATURE TO REMOTE HOST #1
A17
END

FIG. 3

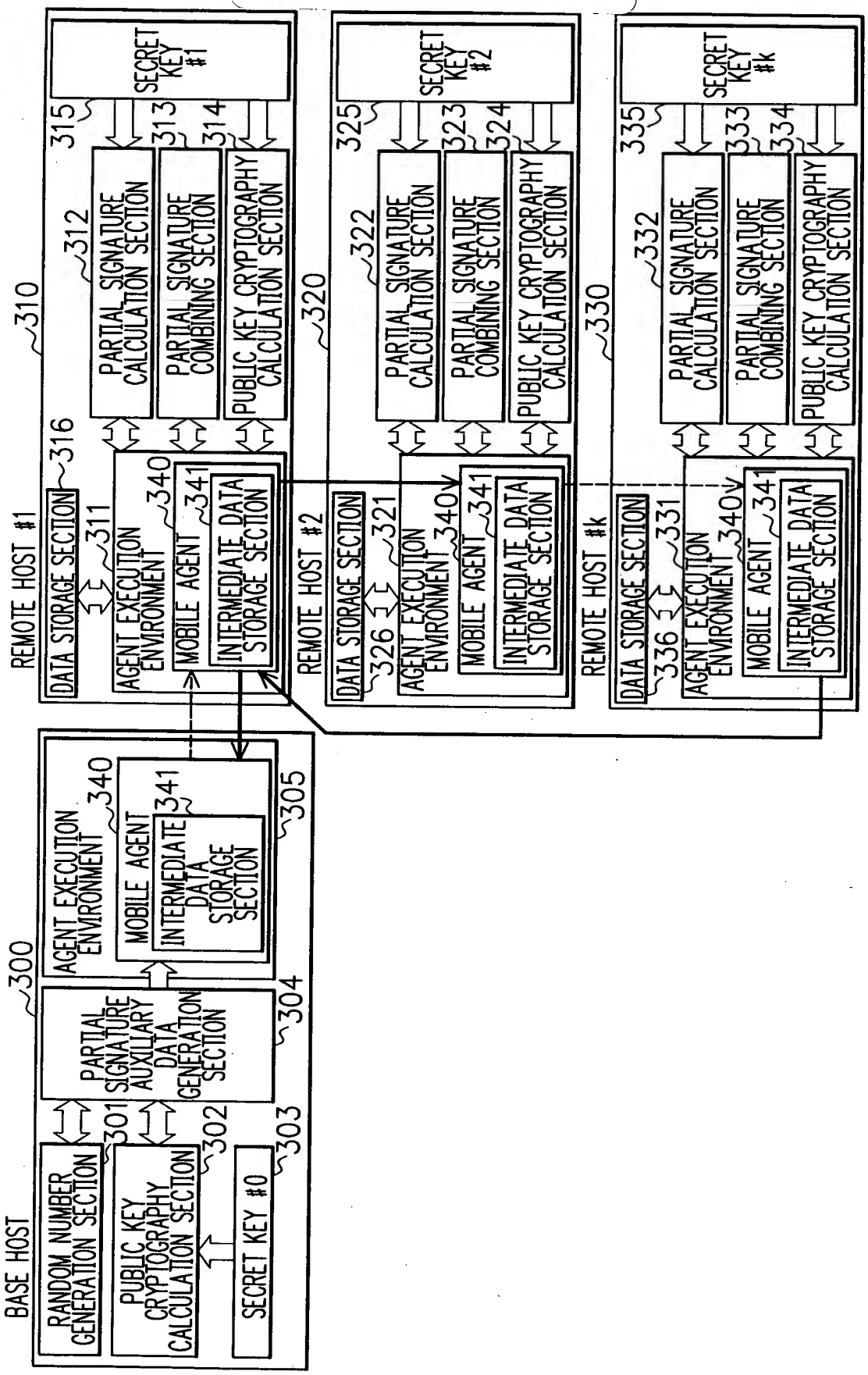

BASE HOST
300
RANDOM NUMBER GENERATION SECTION
301
PUBLIC KEY CRYPTOGRAPHY CALCULATION SECTION
302
SECRET KEY #0
303
PARTIAL SIGNATURE AUXILIARY DATA GENERATION SECTION
304
AGENT EXECUTION ENVIRONMENT
340
MOBILE AGENT
341
INTERMEDIATE DATA STORAGE SECTION
305
REMOTE HOST #1
310
DATA STORAGE SECTION
316
311
AGENT EXECUTION ENVIRONMENT
340
MOBILE AGENT
341
INTERMEDIATE DATA STORAGE SECTION
PARTIAL SIGNATURE CALCULATION SECTION
312
PARTIAL SIGNATURE COMBINING SECTION
313
PUBLIC KEY CRYPTOGRAPHY CALCULATION SECTION
314
SECRET KEY #1
315
REMOTE HOST #2
320
DATA STORAGE SECTION
321
AGENT EXECUTION ENVIRONMENT
340
MOBILE AGENT
341
INTERMEDIATE DATA STORAGE SECTION
PARTIAL SIGNATURE CALCULATION SECTION
322
PARTIAL SIGNATURE COMBINING SECTION
323
PUBLIC KEY CRYPTOGRAPHY CALCULATION SECTION
324
SECRET KEY #2
325
REMOTE HOST #k
330
DATA STORAGE SECTION
331
AGENT EXECUTION ENVIRONMENT
340
MOBILE AGENT
341
INTERMEDIATE DATA STORAGE SECTION
PARTIAL SIGNATURE CALCULATION SECTION
332
PARTIAL SIGNATURE COMBINING SECTION
333
PUBLIC KEY CRYPTOGRAPHY CALCULATION SECTION
334
SECRET KEY #k
335

FIG. 4

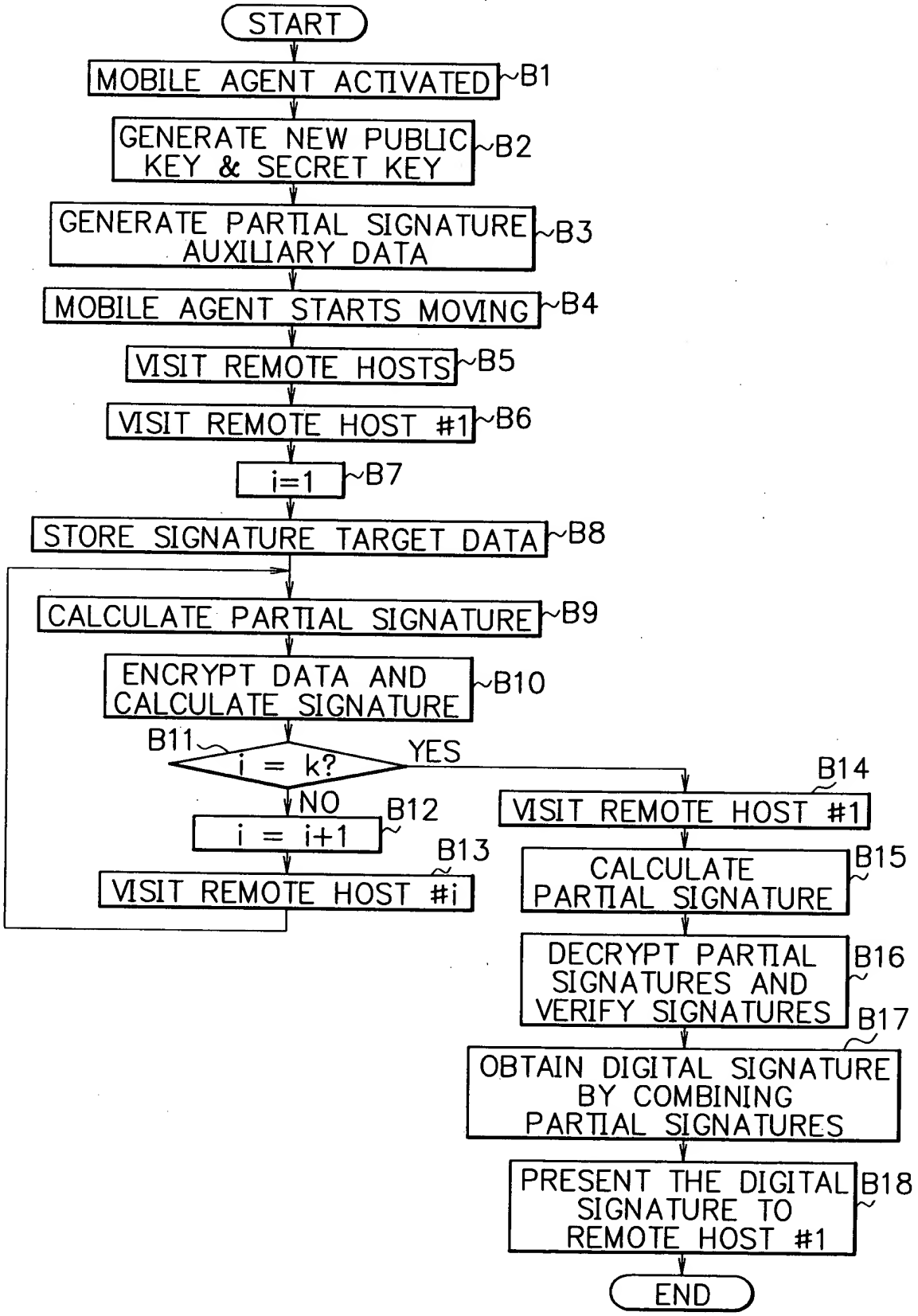
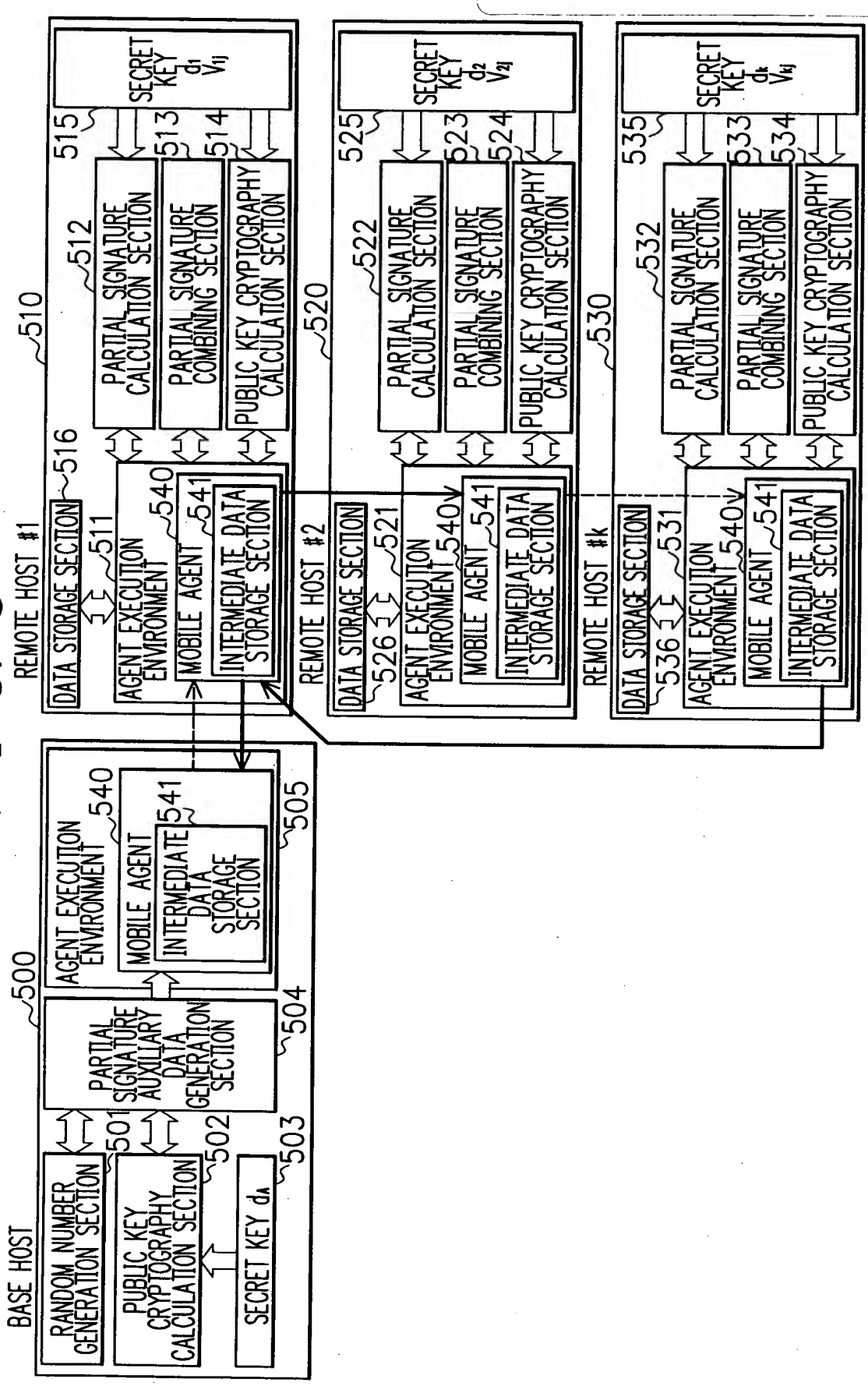
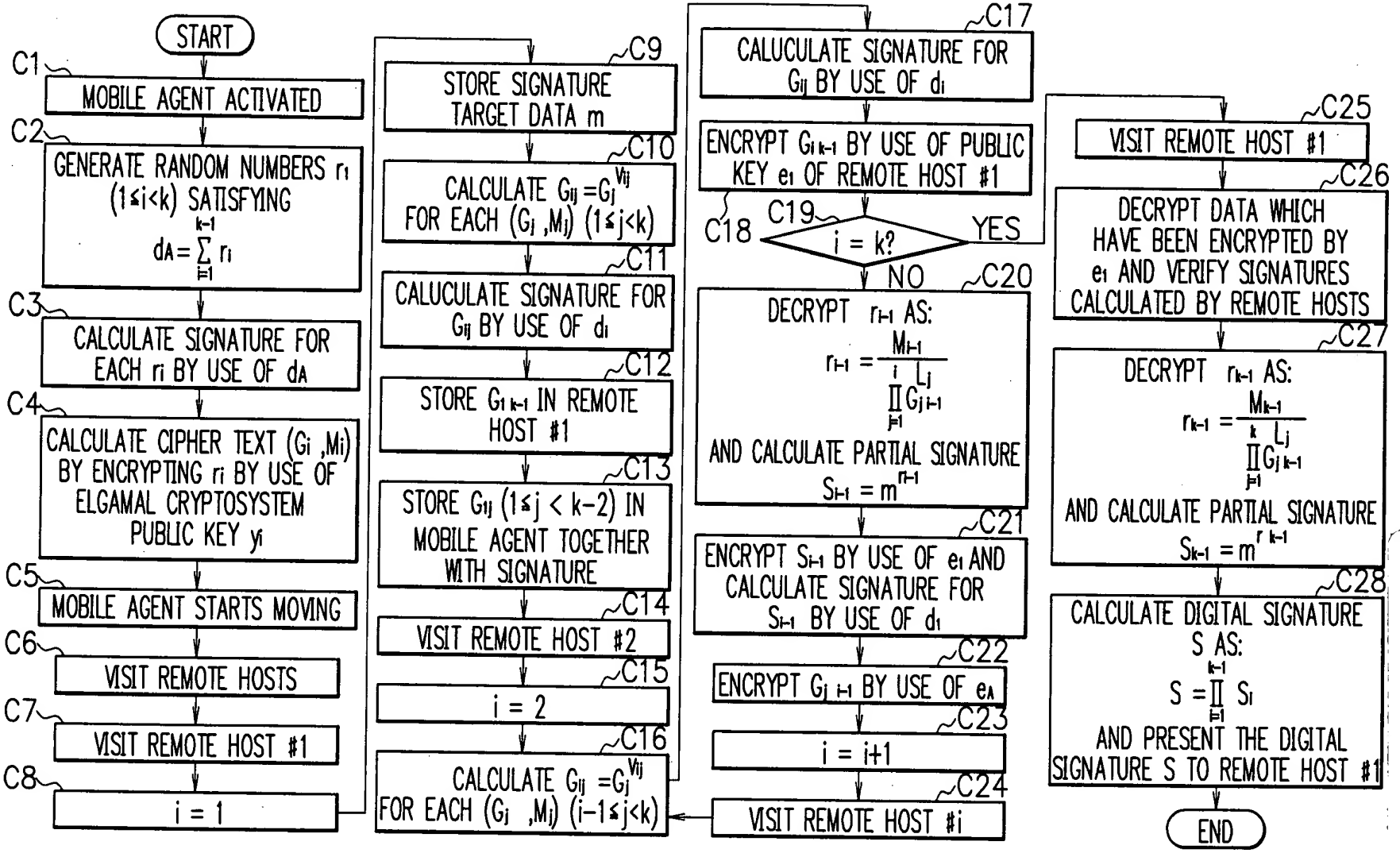

START
MOBILE AGENT ACTIVATED
B1
GENERATE NEW PUBLIC KEY & SECRET KEY
B2
GENERATE PARTIAL SIGNATURE AUXILIARY DATA
B3
MOBILE AGENT STARTS MOVING
B4
VISIT REMOTE HOSTS
B5
VISIT REMOTE HOST #1
B6
i=1
B7
STORE SIGNATURE TARGET DATA
B8
CALCULATE PARTIAL SIGNATURE
B9
ENCRYPT DATA AND CALCULATE SIGNATURE
B10
B11
i = k?
YES
NO
B12
i = i+1
B13
VISIT REMOTE HOST #i
B14
VISIT REMOTE HOST #1
B15
CALCULATE PARTIAL SIGNATURE
B16
DECRYPT PARTIAL SIGNATURES AND VERIFY SIGNATURES
B17
OBTAIN DIGITAL SIGNATURE BY COMBINING PARTIAL SIGNATURES
B18
PRESENT THE DIGITAL SIGNATURE TO REMOTE HOST #1
END

FIG. 5

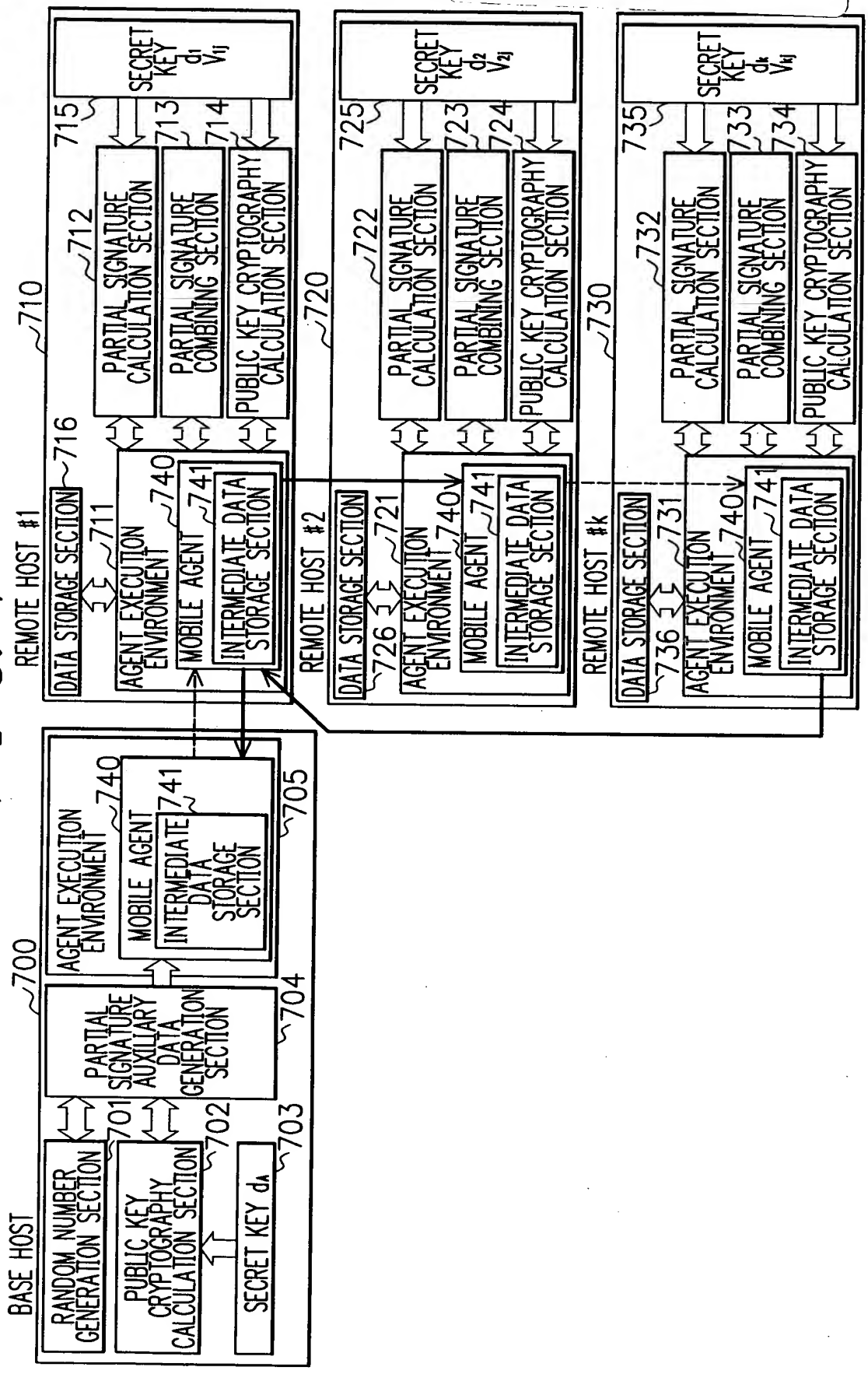

BASE HOST
500
RANDOM NUMBER GENERATION SECTION
501
PUBLIC KEY CRYPTOGRAPHY CALCULATION SECTION
502
SECRET KEY d_A
503
PARTIAL SIGNATURE AUXILIARY DATA GENERATION SECTION
504
AGENT EXECUTION ENVIRONMENT
540
MOBILE AGENT
541
INTERMEDIATE DATA STORAGE SECTION
505
REMOTE HOST #1
510
DATA STORAGE SECTION
516
511
AGENT EXECUTION ENVIRONMENT
540
MOBILE AGENT
541
INTERMEDIATE DATA STORAGE SECTION
PARTIAL SIGNATURE CALCULATION SECTION
512
PARTIAL SIGNATURE COMBINING SECTION
513
PUBLIC KEY CRYPTOGRAPHY CALCULATION SECTION
514
SECRET KEY d_1 V_{1j}
515
REMOTE HOST #2
520
DATA STORAGE SECTION
526
521
AGENT EXECUTION ENVIRONMENT
540
MOBILE AGENT
541
INTERMEDIATE DATA STORAGE SECTION
PARTIAL SIGNATURE CALCULATION SECTION
522
PARTIAL SIGNATURE COMBINING SECTION
523
PUBLIC KEY CRYPTOGRAPHY CALCULATION SECTION
524
SECRET KEY d_2 V_{2j}
525
REMOTE HOST #k
530
DATA STORAGE SECTION
536
531
AGENT EXECUTION ENVIRONMENT
540
MOBILE AGENT
541
INTERMEDIATE DATA STORAGE SECTION
PARTIAL SIGNATURE CALCULATION SECTION
532
PARTIAL SIGNATURE COMBINING SECTION
533
PUBLIC KEY CRYPTOGRAPHY CALCULATION SECTION
534
SECRET KEY d_k V_{kj}
535

F I G. 6



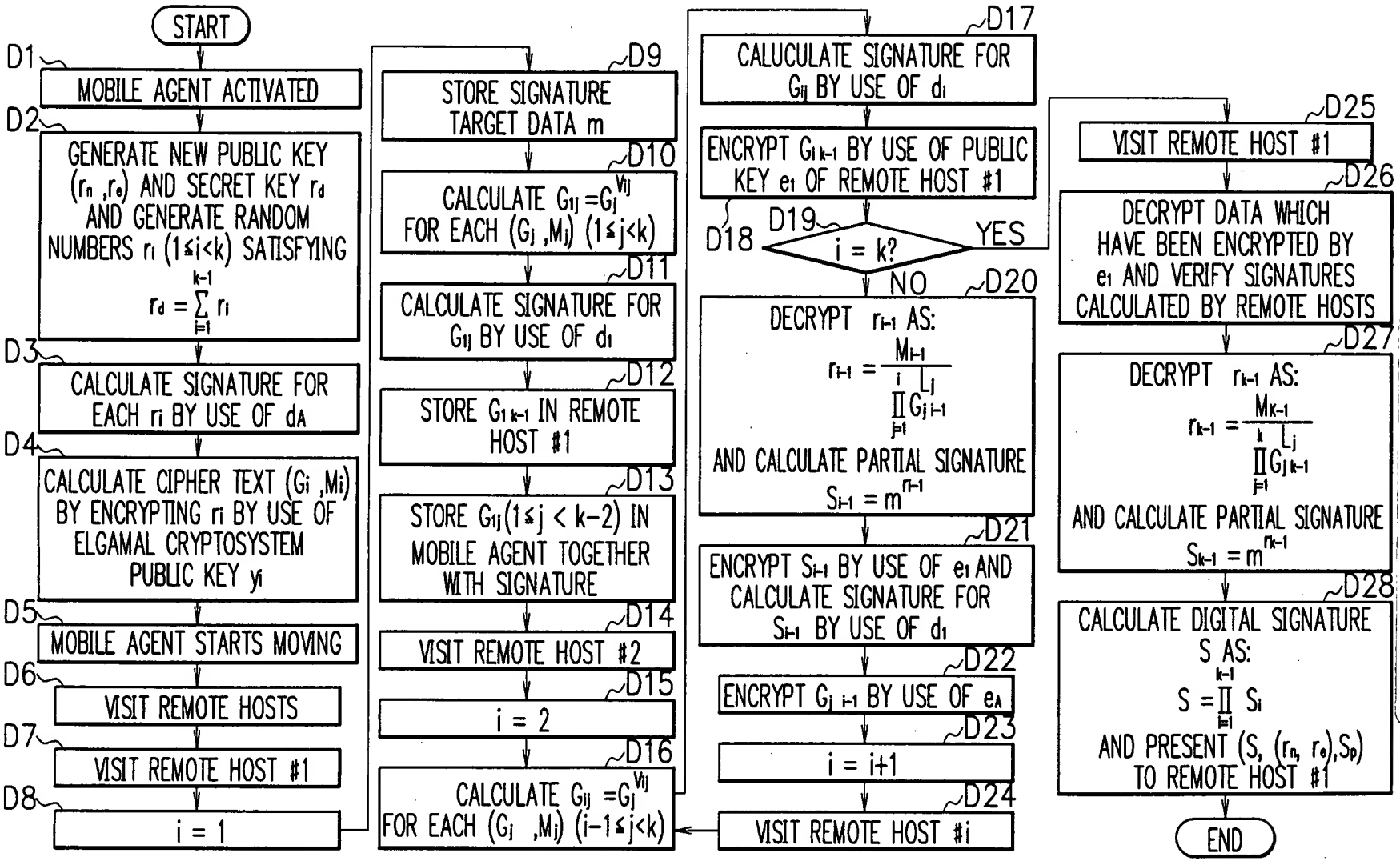
Title: SIGNATURE CALCULATION SYSTEM BY USE OF MOBILE AGENT
Inventor(s): Satoshi OBANA
DOCKET NO.: 072982/0214
Sheet 6 of 8

FIG. 7


BASE HOST
700
RANDOM NUMBER GENERATION SECTION
701
PUBLIC KEY CRYPTOGRAPHY CALCULATION SECTION
702
SECRET KEY d_A
703
PARTIAL SIGNATURE AUXILIARY DATA GENERATION SECTION
704
AGENT EXECUTION ENVIRONMENT
740
MOBILE AGENT
741
INTERMEDIATE DATA STORAGE SECTION
705
REMOTE HOST #1
710
DATA STORAGE SECTION
716
711
AGENT EXECUTION ENVIRONMENT
740
MOBILE AGENT
741
INTERMEDIATE DATA STORAGE SECTION
PARTIAL SIGNATURE CALCULATION SECTION
712
PARTIAL SIGNATURE COMBINING SECTION
713
PUBLIC KEY CRYPTOGRAPHY CALCULATION SECTION
714
SECRET KEY d_1 V_{1j}
715
REMOTE HOST #2
720
DATA STORAGE SECTION
721
AGENT EXECUTION ENVIRONMENT
740
MOBILE AGENT
741
INTERMEDIATE DATA STORAGE SECTION
PARTIAL SIGNATURE CALCULATION SECTION
722
PARTIAL SIGNATURE COMBINING SECTION
723
PUBLIC KEY CRYPTOGRAPHY CALCULATION SECTION
724
SECRET KEY d_2 V_{2j}
725
REMOTE HOST #k
730
DATA STORAGE SECTION
731
AGENT EXECUTION ENVIRONMENT
740
MOBILE AGENT
741
INTERMEDIATE DATA STORAGE SECTION
PARTIAL SIGNATURE CALCULATION SECTION
732
PARTIAL SIGNATURE COMBINING SECTION
733
PUBLIC KEY CRYPTOGRAPHY CALCULATION SECTION
734
SECRET KEY d_k V_{kj}
735

Docket Number

F I G. 8



Title: SIGNATURE CALCULATION SYSTEM BY USE OF MOBILE AGENT
Inventor(s): Satoshi OBANA
DOCKET NO.: 072982/0214
Sheet 8 of 8